Title	SAS-2 を用いた複数端末認証可能なセキュア公衆無線 LAN 通信の研究
Author(s)	横山，拓磨
Citation	
Date of issue	2018-03
URL	http://hdl.handle.net/10173/1916
Rights	
Text version	author

平成 29 年度

修士学位論文

SAS-2 を用いた複数端末認証可能なセキュア公衆無線 LAN 通信の研究

Research on Secure Public Wireless LAN Communication with Multiple devices Authentication Using SAS-2

1205088　　横山 拓磨

指導教員　　清水 明宏

2018 年 2 月 28 日

高知工科大学大学院 工学研究科 基盤工学専攻

情報システム工学コース

要 旨

SAS-2 を用いた複数端末認証可能な セキュア公衆無線 LAN 通信の研究

横山 拓磨

近年，公衆無線 LAN サービスが多くの場所で提供されている．また，訪日外国人を増加させるための政策として，観光地でのアクセスポイントの設置が進められ，年々アクセスポイントが増加している．しかし，これらの公衆無線 LAN サービスの多くは，ノンパスワード，共通のパスワードを使用するものであり，不特定多数の利用者が使用する環境では，第三者による盗聴，改竄などの中間者攻撃の危険性がある．この問題に対処する方式として，SAS-VPN がある． SAS-VPN は，他の VPN 方式の比較評価が行われていないため有用性が示されていない点や，一つの ID を用いて複数の端末認証を行うことができない．本研究では、複数端末認証可能にした SAS-VPN を提案し、HTTPS 通信や VPN 方式で評価し、その有用性を示す。

キーワード　公衆無線 LAN，VPN，認証，SAS-2，複数端末

Abstract

Research on Secure Public Wireless LAN Communication with Multiple devices Authentication Using SAS-2

YOKOYAMA Takuma

In recent years, public wireless LAN service has been provided in many places. In addition, as a policy to increase the number of foreign visitors to Japan, the installation of access points at tourist spots has progressed, and access points are increasing year by year. However, most of these public wireless LAN services use non-passwords and common passwords, and in an environment used by an unspecified number of users, it is difficult for third parties to intercept attacks such as eavesdropping and tampering There is a risk. As a method to deal with this problem, there is SAS-VPN. SAS-VPN can not perform multiple terminal authentication using one ID, because usefulness is not shown because comparison evaluation of other VPN method is not performed. In this research, we propose SAS-VPN which made multiple terminal authentication possible, evaluated by HTTPS communication and VPN method, and show its usefulness.

key words Public Wireless LAN, VPN, Authentication, SAS-2, Multiple devices

目次

目次

図目次

表目次

第 1 章

はじめに

1.1 背景

近年，駅や街中など多くの場所で公衆無線 LAN(Local Area Network) サービスが提供されている．また，政府による ICT 関係重点政策の一つとして, 観光客の利便性を向上させるため，公衆無線 LAN 環境の整備が推進され，多くの自治体などで独自の公衆無線 LAN サービスの提供や無線基地局 (アクセスポイント) が設置されている [1]. これらの公衆無線 LAN サービスは，Wi-Fi(Wireless Fidelity) 規格に対応する機器であれば利用できる．

しかし，利用者の利便性を考慮し，通信の暗号化の設定がされていないものや，共通のパスワードを利用し提供をしているものが存在し，このようなアクセスポイントを利用した場合，第三者による，データの盗聴や改竄などの中間者攻撃の危険性があるため，安全ではない．また，正規のアクセスポイントと同一 SSID を用いた偽装アクセスポイントの問題もある．偽装アクセスポイントの問題では，データの盗聴や改竄などの危険性だけでなく，偽装した経路情報を用いたファーミングによる，偽造サイトへの誘導の危険性も存在する [6].

また，公衆無線 LAN サービスを安全に利用する方式として遠藤により，ワンタイムパスワード相互認証方式 SAS-2(Simple And Secure password authentication protocol, ver.2)[**?**] と VPN を組み合わせた SAS-VPN が提案された [4]．しかし，方式のみの提案で，公衆無線 LAN で安全に通信を行うことのできる他の VPN 方式や SSL/TLS(Secure Sockets Layer/Transport Layer Security) を用いた HTTPS 通信との評価がされていない．また，提案では，認証時に必要な情報を端末内に保存しているため複数端末による認証を行う事が出来ない．そのため，複数端末による認証を行う方式として古田に提案された情報を

端末内ではなくサーバへ保存する方式 [5] を用いる必要がある．しかし，サーバに保存しておく方式では，ID/パスワードが漏洩した場合，容易になりすましが可能となる．

そのため，本研究では，複数端末での認証を可能にし，ID/パスワードが漏洩した場合であっても，なりすましを容易に行うことができない，安全な公衆無線 LAN 通信の提案を行う．最後に，本研究における方式を用いた VPN 方式を実装し，検証および評価を行う．

1.2　本論文の概要

本論文では，複数端末での認証を可能にし，ID/パスワードが漏洩した場合であっても，なりすましを容易に行うことができない，安全な公衆無線 LAN 通信を目指す研究について述べる．

2 章では，無線 LAN の概要，現在運用されている公衆無線 LAN 通信サービスの概要，サービスの問題点について述べる．および，問題点の対策について述べる．

3 章では，VPN の鍵共有を行う方式である IKE，SSL/TLS，ワンタイムパスワード認証方式 SAS-2，複数端末可能にした SAS-2 方式について述べる．4 章では，ID/パスワードが漏洩した場合であっても，なりすましを容易に行うことができない，複数端末認証可能 SAS-2 方式について述べる．5 章では，提案方式を実装を行う．また最後に，本論文の成果と今後の課題について述べる．

第 2 章

公衆無線 LAN サービスの現状

本章では，無線 LAN の概要，現在運用されている公衆無線 LAN 通信サービスの概要，サービスの問題点について述べ，サービスの問題を解決する HTTPS 通信と VPN について述べる．

2.1 無線 LAN

無線 LAN とは，IEEE802.11 規格に準拠する機器で構成されたネットワークのことを指す. 機器同士の通信を無線で行うため，有線 LAN と比べ，ネットワークに接続する際に，LAN ケーブルを使用しない．このことから，無線 LAN を用いる場合，移動する通信機器との接続が容易に行え，ネットワークの提供が，有線 LAN に比べ，ネットワークの提供が行いやすくなる．また，ケーブルの必要がないため，運用コストや物理コストを抑えることができる．近年では，アクセスポイントやクライアント端末の相互認証を保証した無線 LAN 機器の普及が進んでいる．

2.2 公衆無線 LAN サービスの特徴

公衆無線 LAN サービスとは，無線 LAN を利用し，インターネットへの接続を提供するサービスのことである．主な提供場所は，人の集中する商業施設や公共機関，宿泊施設，観光地の施設等である．利用者は無線 LAN の規格に対応したパソコンやスマートフォンを用いることにより利用できる．

また，近年，クルーズ船の寄港増加や航空路線の拡大などにより訪日外国人が増加してお

り，訪日外国人獲得の政策として，全国の自治体で，公衆無線 LAN サービスの提供が行われている．図 2.1 は 2011 年から 2017 年までの訪日外国人数である．

．また，総務省の ICT(Information and Communication Technology) 重点政策として，

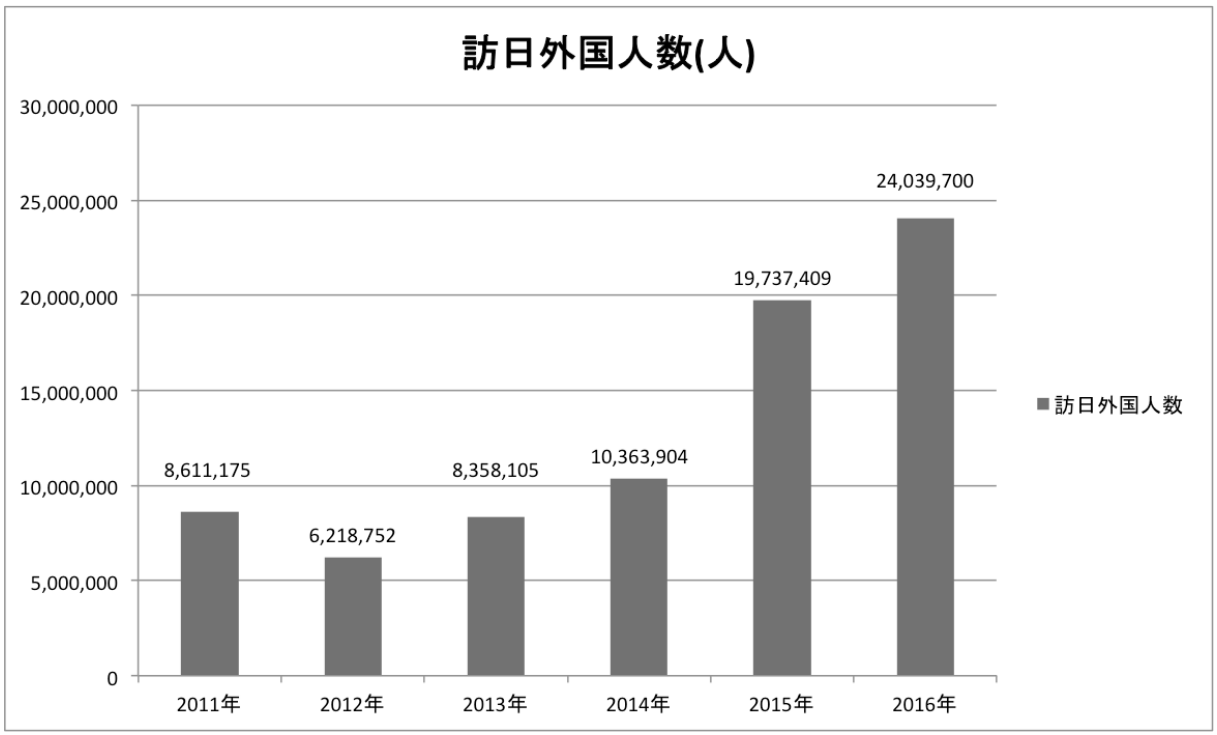

図 2.1　訪日外国人数

ICT による地域活性化，2020 年に開催されるオリンピック・パラリンピック東京大会へ向けた施策として全国で公衆無線 LAN サービスが整備が推進されアクセスポイントが増加している．自治体で運用される公衆無線 LAN サービスには以下のような特徴がある．

- 無料
- 異なるアクセスポイントでの同一 SSID
- 簡易的な利用者登録
- ID/パスワードの配布・掲載

2.3　公衆無線 LAN サービスの問題点

公衆無線 LAN 通信では，利用者の利便性，サービス提供の容易性などを確保するため，無線で広範囲利用できる様になっている．しかし，広範囲に電波が届くため，通信可能範囲内であれば利用者以外でもその電波を受信することが可能である．そのため，第三者から通信データの盗聴，改竄等の中間者攻撃の危険性がある状況となっている．公衆無線 LAN サービスのような広範囲かつ，不特定多数の利用者がいる環境では以下の 3 つのような危険性がある [6].

2.3.1　ノンパスワード

サービスの利用者の利便性を考慮して，通信データを行わないものが存在する．暗号化行わないため，管理者がパスワードを配布する手間や，利用者がパスワードの入手，入力などの手間を省くことができることから，負担を軽減することができる．しかし，通信データが暗号化されないため，広域にデータを送信してしまう無線 LAN 通信の特性上，第三者による盗聴，改竄等の危険性が非常に高くなってしまう．

2.3.2　共通パスワード

無線 LAN の暗号方式として認証サーバを必要のない安全な接続方式として WPA2-PSK がある．パスワードは．事前共有鍵の役割を持ちその情報を元に鍵の生成，通信の暗号化を行う．そのため，パスワードを入手することが可能なら，誰でも暗号化されたデータの復号を行うことができる．その結果，第三者による通信データの盗聴，改竄等の中間者攻撃を受ける危険性がある．

2.3.3　偽装 SSID(なりすましアクセスポイント)

無線 LAN サービス利用者の利便性を考慮し，どのアクセスポイントでも同一の SSID が用いられることが多い．また，サービスの特性上，SSID のは利用者以外でも知ること可能

である．そのため，第三者が同一の SSID を用いて，偽装した SSID を用いて偽装したアクセスポイントを設置することが可能で，この偽アクセスポイントに接続した場合，利用者が通信内容の盗聴，改竄という危険性がある．

また，偽装の経路情報を持つ DNS サーバへアクセスさせ，利用者の利用する Web ページに似たページを作成し，正規の Web サイトのログインに必要な ID/パスワード等の情報を入力させ，不正に情報を入手するファーミングという攻撃の危険性もある＼ [7]．この様なアクセスポイントが存在する場合，利用者にとって，利用するアクセスポイントが正規のものであるのか，偽装されたものであるのかを判断することは困難である．

2.4　公衆無線 LAN でのセキュア通信

危険性への対策として，HTTPS の利用や VPN の利用がある．

2.4.1　HTTPS

安全に Web サイトを閲覧する方法として，SSL/TLS プロトコルを用いた HTTPS 通信がある．HTTPS 通信では，SSL/TLS プロトコルを用いることにより，通信を行うサーバの認証や通信内容の暗号化，改竄検出を行う．HTTPS は，OS が標準搭載しているブラウザなどから簡単に接続でき，利用者は手間がなく利用することができる．利用者はブラウザの URL が「https:」となっていることを確認することで HTTPS 通信が行われているかを確認することができる．

HTTPS 通信の問題として，ユーザは，アクセスしたい Web サイトが HTTPS を用いない場合，暗号通信を行うことができない．また，偽装した SSID を用いたアクセスポイントへ接続してしまった場合，通信内容の盗聴，改竄等の危険は防ぐことができるが，DNS を用いて接続先の IP アドレスを求めるため，偽装経路情報を用いたファーミングを行われる危険性はある．管理者側では HTTPS を行うためにサーバ証明書を用いるが，証明書の発行などの管理コストが発生する．

2.4.2　VPN

公衆無線 LAN サービスのような環境下で，利用者が安全に通信を行う方法として VPN がある．VPN とは，インターネットなどのパブリックなネットワーク上でプライベートネットワークを構築すること，またはそれらのサービス，技術のことである [8].

プライベートネットワーク内での通信は，ネットワーク内で予め決められた IP アドレスやプロトコルを用いて通信を行うため，インターネットなどのパブリックネットワークを用いて行う際，そのままデータのやり取りをしてもプロトコルの違いから通信を正常に行うことができない．そこで，VPN の構築のために，通信プロトコルを他の通信プロトコルのパケット内に包み込むカプセル化を用いて行われる．通信環境上に異なるプロトコルを透過させる方法をトンネリングという．VPN の接続方式には大きく分けた，拠点間通信とリモートアクセスの 2 種類に分けることができる，拠点間通信での VPN は離れた LAN 同士を接続するものである．それに対しリモートアクセスは，遠隔地のクライアントコンピュータへの接続を行う．VPN では，VPN 装置でパケットのカプセル化を行い，拠点間に仮想のトンネルを構築する．VPN の方式として，IPsec-VPN，PPTP，L2TP/IPsec，OpenVPN がある．また，遠藤によって提案された SAS-VPN も存在する．

IPsec-VPN

IPsec とは，IP パケット単位で改竄改竄検知やデータの秘匿を行うプロトコルである IPsec を VPN に利用する方式である [**?**]IPsec は，サーバと接続する端末で IKE(Internet Key Exchange) による認証，鍵共有する．ESP(Encapsulating Security Payload) による通信の暗号化と完全性の検証．または，AH (Authentication Header) による完全性の検証を行う．IPsec は，IP 層におけるプロトコルであるため，使用するアプリケーションを限定することなく，通信経路上の通信内容の盗聴，改竄を防ぐことが可能である．IPSec では，AES 等の強固な暗号方式を用いて通信が行えることから安全性が高い．

PPTP

PPTP(Point to Point Tunneling Protocol) とは，PPP(Point-to-Point Protocol) パケットを GRE(Generic Routing Encapsulation) でカプセル化し，PPTP サーバと接続機器の間で PPP 接続するための方式である [**?**]．PPTP で用いられる暗号方式 MEPPMPPE(Microsoft Point to Point Encryption) は暗号化の強度が弱いため，セキュリティ強度に問題がある．

L2TP/IPSec

L2TP は，PPTP と L2F の仕様を統合したものである．PPTP と同様 IP 以外のプロトコルに対応する．しかし，L2TP は暗号化機能を持たないため通信の暗号化に他の技術を併用する必要がある．そのため，一般的に IPsec との組み合わせて利用する．L2TP/IPsec では，L2TP で生成されたパケットを IPsec で暗号化を行うことにより，機密性，完全性を持つ安全な通信を行うことができる [11]．IPsec を用いているため，AES 等の強固な暗号方式を用いて通信が行えることから安全性が高い [11].

また，通信時に L2TP,IPsec の両方のプロトコルを用いるため，ヘッダ増加に伴うオーバヘッドの増加がある．

OpenVPN

OpenVPN は，SSL/TLS プロトコルと OpenSSL ライブラリを用いて安全な VPN 通信を行うためのシステムである．OpenVPN では Ethernet フレームをカプセル化し通信を行う．そのため，任意のアプリケーションで通信を行うことができる．また，標準では UDP 1194 番ポートで通信を行うがサーバの設定で容易に変更を行える．そのため，ファイアウォールの影響を受けることが少ない．しかし，OpenVPN は，標準搭載されている機器がないため，クライアントソフトをインストールしなければならない．

2.4.3　SAS-VPN

SAS-VPN は，ワンタイムパスワード相互認証方式 SAS-2 を用いて VPN を構築する方式である [4] ．SAS-2 を用いることによりユーザと VPN サーバの相互認証，認証毎に更新される認証情報を用いた暗号化鍵更新が行え，安全性の高い通信を行うことができる．SAS-VPN はクライアントソフトが必要となる．

2.5　暗号化鍵の共有方法

この章では，IPsec-VPN，L2TP/IPsec で用いられる IKE と OpenVPN で用いられる SSL/TLS の鍵共有方法を述べる．最後に SAS-VPN で用いられる SAS-2 と，複数台数認証可能にした SAS-2 方式について述べる．

2.5.1　IKE

IKE とは，通信相手の認証，共通鍵の共有，更新を行う方式である [12]．IPsec,L2TP で用いられる．

IKE では，UDP の 500 番ポートを用いて行う．IKE には IKEv1 と IKEv2 の 2 つのバージョンがある．最新のバージョンである IKEv2 を示す．IKE では，通信相手の認証，SA(Security Association) と管理，共通鍵の管理を提供する．IKE では IKE_SA_INIT および IKE_AUTH,CHILD_SA と呼ばれる 3 つのフェーズを行い暗号鍵の共有を行う．IKE_SA_INIT は,IKE_SA と呼ばれる IKE で通信される情報の暗号化を行う為の共通鍵を生成するフェーズである．IKE_AUTH では通信相手の認証と CHILD_SA の折衝を行うフェーズである．CHILD_SA は，IKE 以外の暗号通信するためのフェーズである．IKE の通信概要を図 2.2 に示す．

IKE_SA_INI は，IKE_SA と呼ばれる IKE で通信される情報の暗号化を行う為の共通鍵を生成する．IKE_SA_INI では，暗号方式の選択・決定し，鍵生成情報を共有することにより、暗号鍵を共有し，IKE_SA を構築する．

2.5　暗号化鍵の共有方法

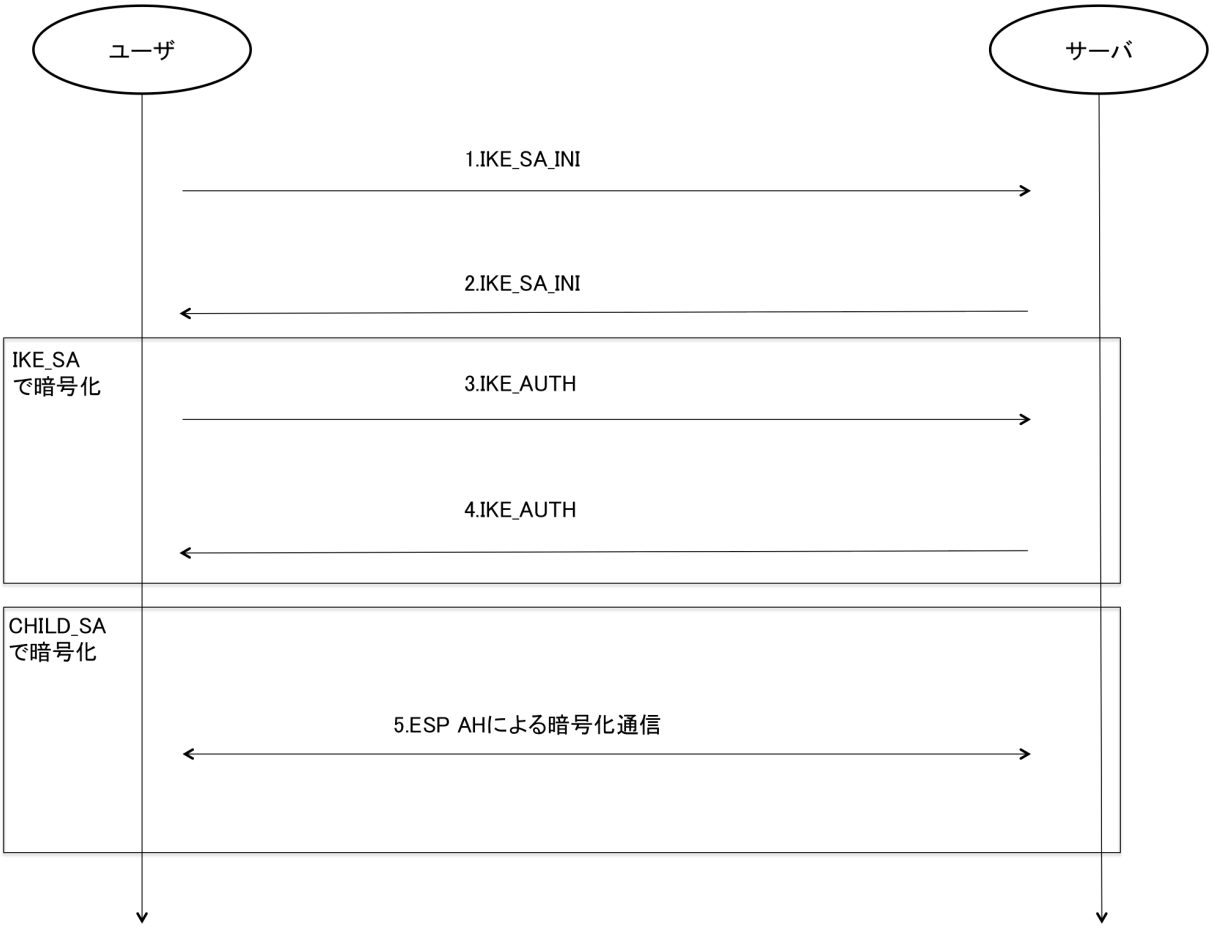

図 2.2　IKE 通信概要

IKE_AUTU では，IKE_SA_INI で生成した共通鍵を用いて通信を行う．

IKE_AUTH は，認証情報，CHILD_SA を確立するために用いる共通鍵方式の共有を行う．認証方式は事前鍵共有方式，証明書方式がある．IKE_AUTH では，共通鍵方式の決定を行い，使用する共有鍵方式の通知, ナンス，認証情報を送信する．

この手順により安全に IPsec で用いる共通鍵の共有と認証を行うことができる．

IKE では，事前鍵共有方式の鍵管理コスト，証明書の管理コスト，ファイアウォールの透過不可の 3 つ問題が存在する．1 つ目は，事前鍵共有方式の鍵管理コストの問題である．事前鍵を用いる方式で，接続するユーザ毎に事前鍵を生成する必要があり，接続されるユーザが増加した場合に，鍵管理コストがかかる．2 つ目は証明書の管理コストの問題である．証明書を発行・更新などの管理が必要となるため，管理コストがかかる．3 つ目は，使用ポー

トが UDP の 500 番ポートを用いて行うため，ファイアウォールでの拒否が行われ通信が行えない．

2.5.2　SSL/TLS

SSL/TLS とは，公開鍵暗号方式と共痛鍵暗号方式方式の両方を用いたハイブリット暗号方式である．共有鍵の共有に公開鍵を用いて行い，鍵交換後は共通鍵を用いて通信を行う．このため，盗聴やなりすましに強い，一方向性関数を用いており改竄検知も可能である．SSL/TLS では，公開鍵を用いて通信を行っているため，証明書を公開鍵を電子証明書，認証局を用いる必要性がある．そのため，証明書の発行や運用にコストがかかる．SSL/TLS の通信概要を図 2.5 に示す．SSL/TLS の手順を説明する．

1. サーバは公開鍵・秘密鍵の生成を行う
2. 公開鍵と各証明書を認証局に送信する
3. 認証局でサーバから送られてきた情報を審査し．認証局の生成した秘密鍵でサーバの公開鍵を暗号化し，証明書を発行する．
4. ユーザは認証局の公開鍵である証明書を事前にインストールする．
5. ユーザがサーバへ接続要求を行った際にサーバの証明書をユーザに送信する．
6. ユーザは受信した証明書を認証局の公開鍵で復号し，サーバの検証を行う．
7. ユーザは乱数を生成し，サーバの公開鍵で暗号化し，送信を行う．
8. ユーザ乱数から共有鍵を生成する．またサーバは情報を秘密鍵で復号し，鍵の生成を行う．

2.5.3　ワンタイムパスワード相互認証方式 SAS-2

ワンタイムパスワード相互認証方式 SAS-2 は，証明書を用いることなく安全に相互認証，暗号鍵共有を行うことができる方式である．SAS-2 は，初期登録フェーズと認証フェーズで構成される．初期登録フェーズは，1 度のみ実行される．認証フェーズは認証がユーザがロ

2.5　暗号化鍵の共有方法

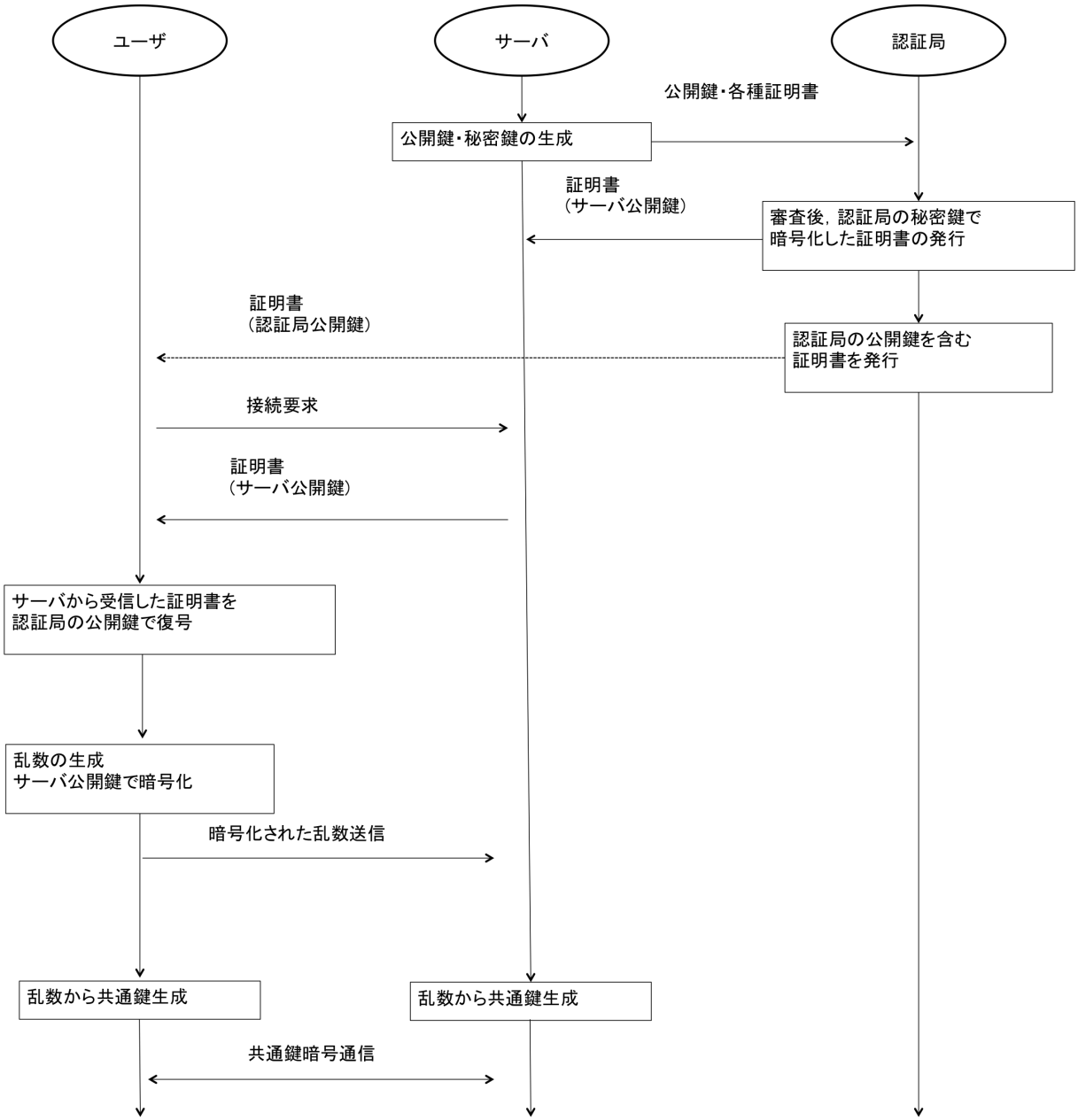

図 2.3　SSL/TLS 概要

グインを行うたびに実行される．

定義と記法

- User は，認証されるユーザである．

- Server は，User を認証する認証者である．
- Uid はユーザの識別子を示す.
- P はユーザのパスワードを示す.
- i は, 認証セッション毎に加算される数値である.
- N_i は，i 回目の認証時に生成される乱数を示す
- X，F，H は一方向性関数を示す．例として F(x) は x を一方向性関数に適用して得た出力値を示す．また，この一方向性関数は出力ビット数が常に一定とする.
- +は加算演算子を示す.
- $\oplus$ は, 排他的論理和演算子を示す.
- A,C は認証情報を示す.

初期登録フェーズ

初期登録フェーズでは，まずユーザが認証情報を生成し，安全な経路を用いてサーバへ共有する必要がある．初期登録フェーズの手順を図 2.4 に示す.

1. ユーザは自身の識別情報 Uid とパスワード P を入力する．また，同時に N_0 の生成を行い，$\mathrm{A} = \mathrm{X}(\mathrm{Uid}, \mathrm{P} \oplus N_0)$ を算出する．そして，N_0 を端末内へ保存する.
2. ユーザは Uid と生成した A を安全な経路を用いて送信する.
3. サーバは Uid と A を保存する.

認証フェーズ

認証フェーズでは，まずユーザから認証情報をサーバが受け取り，認証情報の正当性を検証し，ユーザの認証を行う．次にサーバで認証情報を生成し，ユーザへ送信する．受信した認証情報の正当性をユーザが検証し，サーバを認証する．これにより相互認証が可能となる．i 回目の認証手順を図**??**に示す.

2.5 暗号化鍵の共有方法

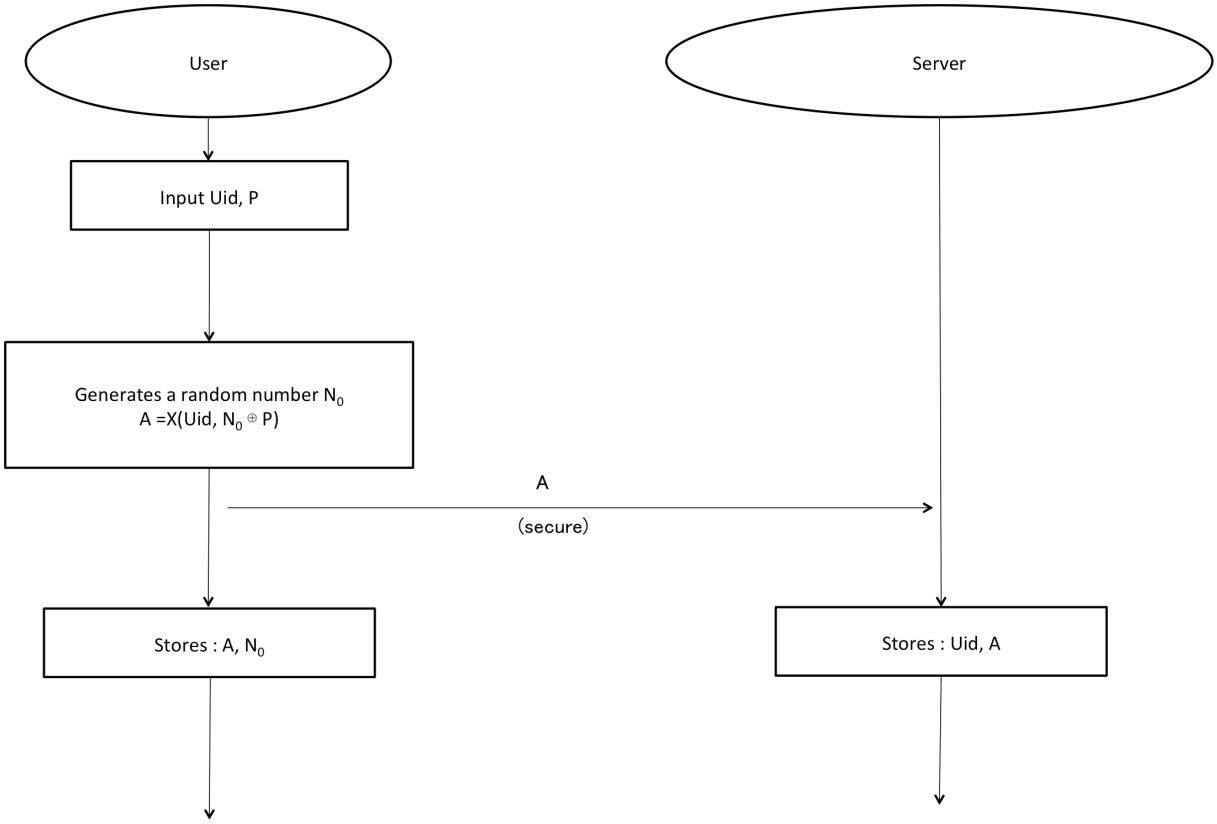

図 2.4 SAS-2 初期登録フェーズ

1. ユーザは自身の識別情報 Uid とパスワード P を入力する．そして，入力された Uid と P，端末に保存してある N_i，A = X(Uid, P $\oplus$ N_i) を算出する．次にユーザは乱数 N_{i+1} を生成し端末へ保存する．さらにユーザは，C = X(ID, P $\oplus$ N_{i+1}) と F(C) = F(ID, C) を算出し， C,F(C) と A を用いて，α = C $\oplus$ (F(C) + A), β = F(C) $\oplus$ A をそれぞれ算出する．
2. ユーザは，サーバへ Uid，α，β，を送信する．この時に用いられる通信はインターネットなどの安全でない通信経路であっても構わない．
3. サーバは受信した β と保存されている A を用いて，F(C) = β $\oplus$ A を算出する．次にサーバは C = α $\oplus$ (F(C) + A) を算出し，F(C) と F(Uid，C) の比較を行う．比較結果が，不一致ならばの認証が不成立となる．一致した場合は認証が成立となる．認証が成立した場合に以下の処理が実行される．

2.5　暗号化鍵の共有方法

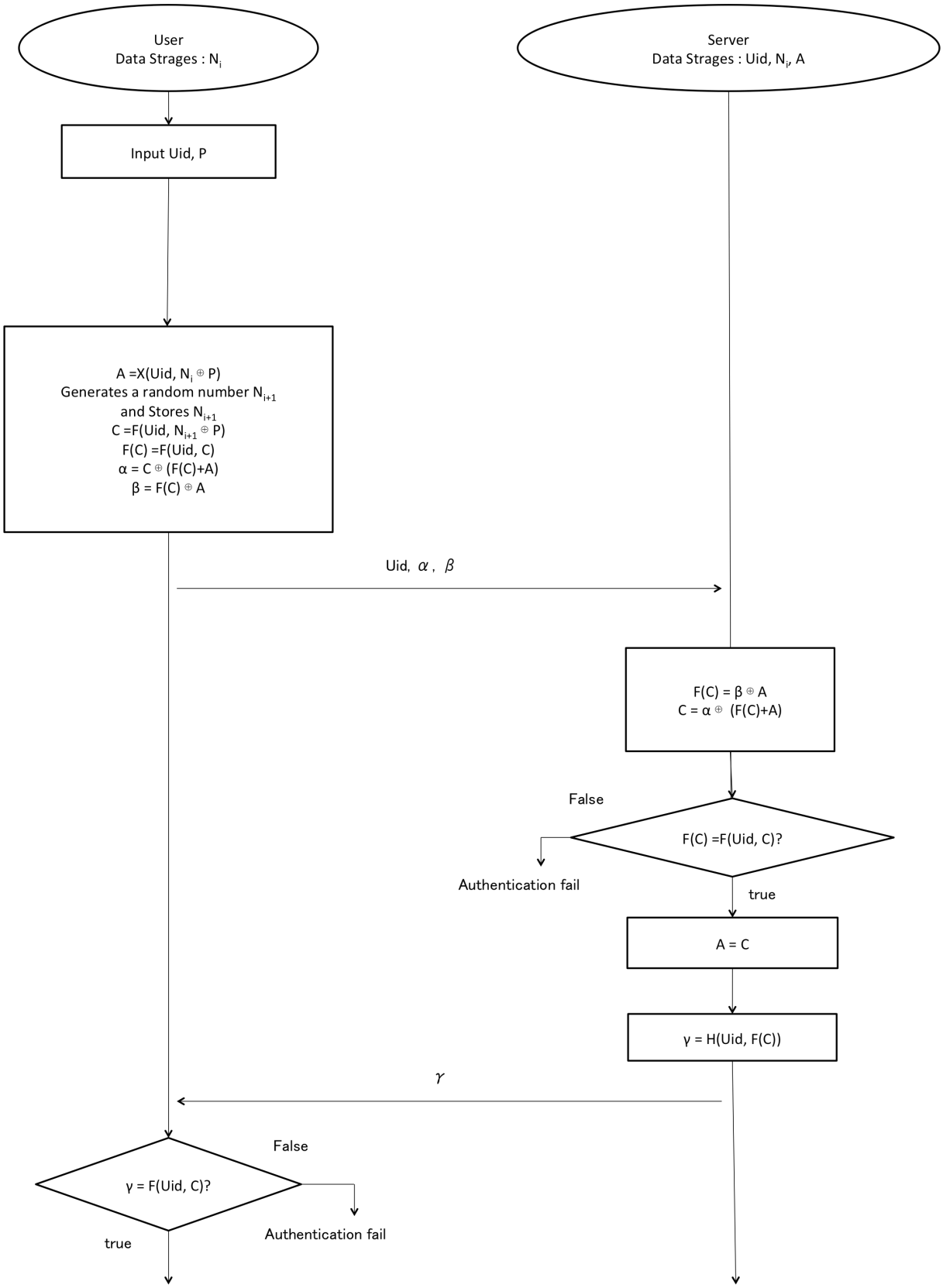

図 2.5　SAS-2 認証フェーズ

4. サーバは，保存された A の代わりに C を保存し，次回認証に備える．さらに γ = H (Uid $\oplus$ F(C)) を生成し，ユーザへ送信する．この時に用いられる通信はインターネットなどの安全でない通信経路であっても構わない．
5. ユーザは H (Uid $\oplus$ F(C)) を算出し，受信した γ と比較を行う．比較結果が，不一致ならばサーバの認証が不成立となる．一致した場合は認証が成立となる．

共有鍵の生成

認証フェーズ終了後，認証情報を鍵生成共有情報とし，共通鍵の生成を行う．このことにより，相互認証と鍵共有を同時に行うことが可能となる．

プロトコルの安全性

ワンタイムパスワード認証方式に対する攻撃法として，反射攻撃によるなりすましが考えられる．反射攻撃では，正当なユーザによる認証が行われた際に送信された情報を，第三者が通信経路上で盗聴し，再利用を行う．正当なユーザが SAS-2 による (i+1) 回目の認証を行う際に，ユーザが送信する情報を以下に示す．

$$\alpha = E \oplus (F(E) + C) \tag{2.1}$$

$$\beta = F(E) \oplus C \tag{2.2}$$

$$ID \tag{2.3}$$

この時，第三者がなりすまし攻撃を実行する場合は，以下の情報を送信しなければならない．

$$\alpha = x \oplus (F(E) + C) \tag{2.4}$$

$$\beta = F(x) \oplus C \tag{2.5}$$

$$ID \tag{2.6}$$

第三者が，たとえ i 回目以前で認証情報を全て取得したとしても，これらの認証情報の組み合わせを生成することは不可能である．このことから SAS-2 プロトコルによる認証は安全であると言える．

問題点

この方式の問題点として複数端末での認証が不可能である．ユーザの ID とパスワードは入力により，他の端末へ共有することができるが，認証情報を生成するための乱数が端末に保存されており，他の端末で認証情報を生成することができない．この方式で複数端末用いる場合には別の Uid を用いて，新たに登録する必要が出てきてしまう．そのため，ユーザは記憶しておく必要のある情報が増えてしまう．

2.5.4　既存複数端末認証可能な SAS-2 方式

SAS-2 認証方式を複数端末認証可能にした方式が古田によって提案された．この方式では，認証情報の生成に用いる乱数を端末ではなく，サーバ側に保存することにより，複数端末での認証を実現する．この方式では，初期登録フェーズと認証フェーズで構成される．初期登録フェーズは，1 度のみ実行される．認証フェーズは認証がユーザがログインを行うたびに実行される．

定義と記法

- User は，認証されるユーザである．
- Server は，User を認証する認証者である．
- Uid はユーザの識別子を示す．
- P はユーザのパスワードを示す．
- i は, 認証セッション毎に加算される数値である．
- N_i は，i 回目の認証時に生成される乱数を示す
- X，F，H は一方向性関数を示す．例として F(x) は x を一方向性関数に適用して得た出力値を示す．また，この一方向性関数は出力ビット数が常に一定とする．
- +は加算演算子を示す．
- $\oplus$ は, 排他的論理和演算子を示す．

- A,C は認証情報を示す.

既存複数端末認証可能 SAS-2 初期登録フェーズ

初期登録フェーズでは，まずユーザが認証情報を生成し，安全な経路を用いてサーバへ共有する．初期登録フェーズを図 2.6 に示す.

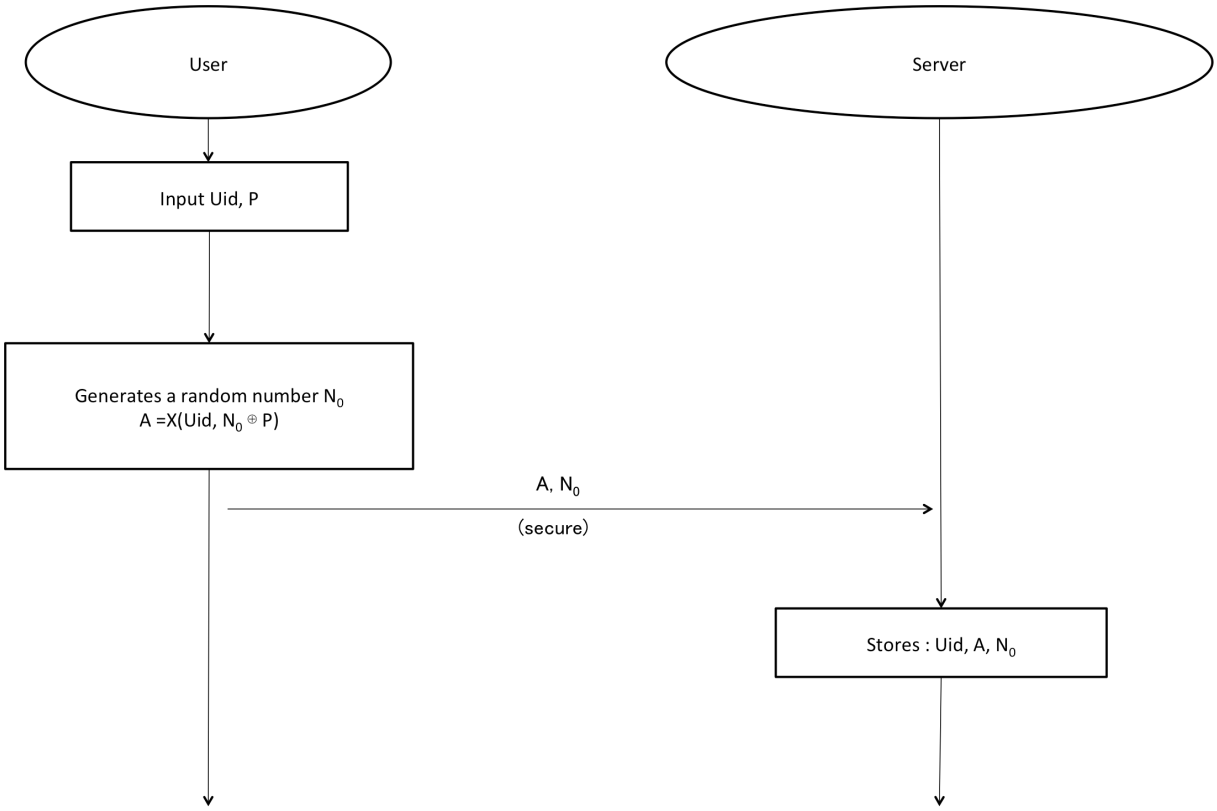

図 2.6　既存複数端末認証可能方式 初期登録フェーズ

1. ユーザは自身の識別情報 Uid とパスワード P を入力する．また，同時に N_0 の生成を行い，A = X(Uid, P $\oplus$ N_0) を算出する.
2. ユーザは Uid と生成した N_0，A を安全な経路を用いて送信する.
3. サーバは Uid と N_0，A を保存する.

既存複数顛末認証可能 SAS-2 認証フェーズ

認証フェーズでは，まずユーザからレスポンスを送信し，サーバからリクエストをとして乱数を送信する．そして，ユーザが認証情報を生成しサーバへ送信する．サーバが受け取り，認証情報の正当性を検証し，ユーザの認証を行う．次にサーバで認証情報を生成し，ユーザへ送信する．受信した認証情報の正当性をユーザが検証し，サーバを認証する．これにより相互認証が可能となる．i 回目の認証手順を図 2.7 に示す.

1. ユーザは自身の識別情報 Uid とパスワード P を入力する.
2. ユーザはサーバへリクエストを送信する.
3. サーバはユーザへレスポンスとして乱数 N_i を送信する
4. Uid と P，受信した N_i，A = X(Uid, P $\oplus$ N_i) を算出する．次にユーザは乱数 N_{i+1} を生成する．そして，ユーザは，C = X(ID, P $\oplus$ N_{i+1}) と F(C) = F(ID, C) を算出し，C,F(C) と A を用いて，α = C $\oplus$ (F(C) + A), β = F(C) $\oplus$ A をそれぞれ算出する.
5. ユーザは，サーバへ Uid，N_{i+1}，α，β，を送信する．この時に用いられる通信はインターネットなどの安全でない通信経路であっても構わない.
6. サーバは受信した β と保存されている A を用いて，F(C) = β $\oplus$ A を算出する．次にサーバは C = α $\oplus$ (F(C) + A) を算出し，F(C) と F(Uid，C) の比較を行う．比較結果が，不一致ならばの認証が不成立となる．一致した場合は認証が成立となる．認証が成立した場合に以下の処理が実行される.
7. サーバは，保存された A の代わりに C の保存と N_i の代わりに N_{i+1} の保存し，次回認証に備える．さらに γ = H (Uid $\oplus$ F(C)) を生成し，ユーザへ送信する．この時に用いられる通信はインターネットなどの安全でない通信経路であっても構わない.
8. ユーザは H (Uid $\oplus$ F(C)) を算出し，受信した γ と比較を行う．比較結果が，不一致ならばサーバの認証が不成立となる．一致した場合は認証が成立となる.

2.5　暗号化鍵の共有方法

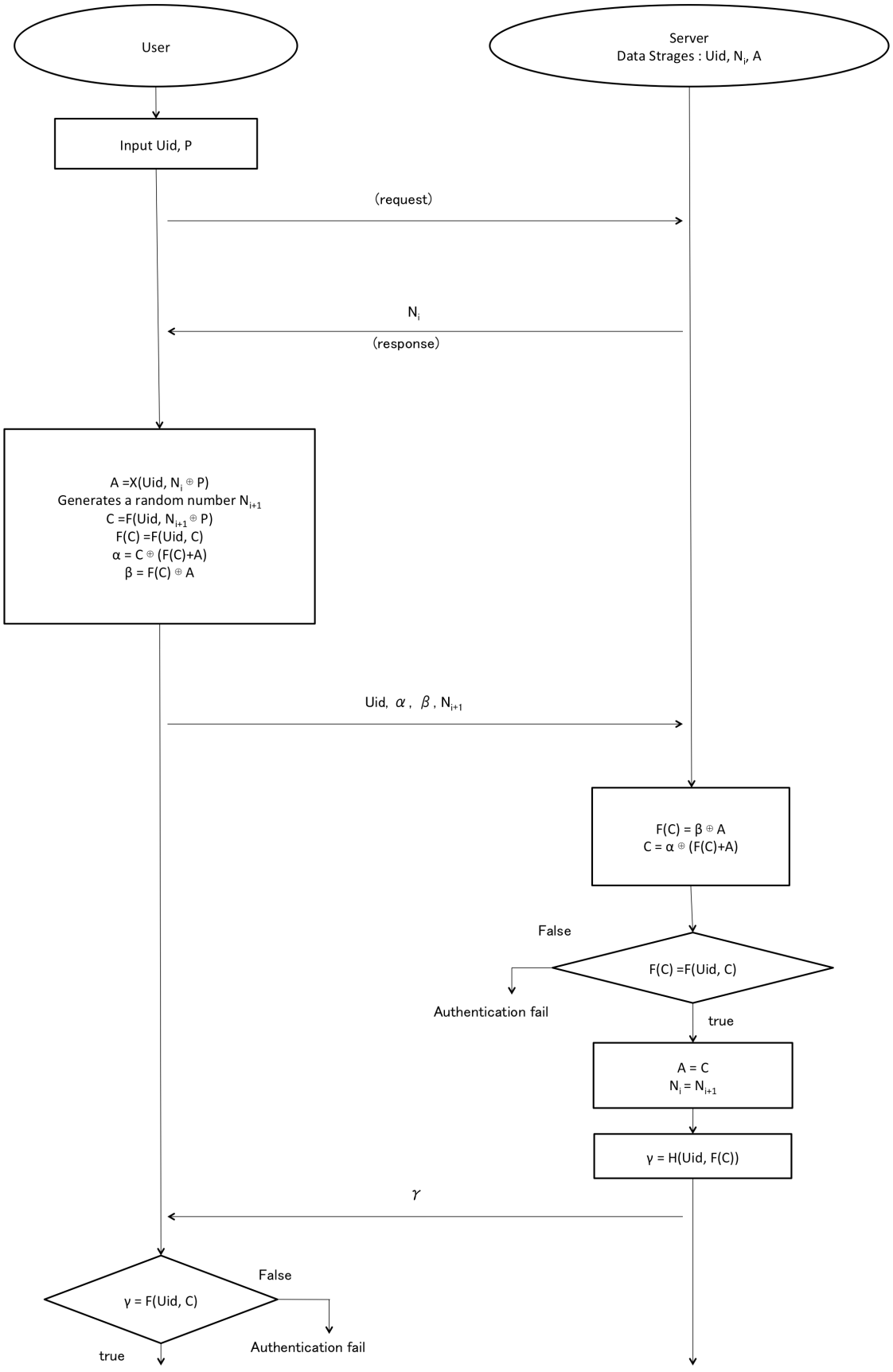

図 2.7　既存複数端末認証可能方式 認証フェーズ

共通鍵の生成

認証フェーズ終了後，認証情報を鍵生成情報とし，共通鍵の生成を行う．このことにより，相互認証と鍵共有を同時に行うことが可能となる．

問題点

この方式の問題点として，アカウントリスト攻撃により，ユーザの ID とパスワードが漏洩した場合，なりすましが可能である．乱数を端末に保存しておく場合，第三者に ID とパスワードが漏洩してしまった場合であっても，第三者から乱数が不明であるため，なりすましを行うことが不可能である．しかし，複数端末認証が可能方式では乱数を取得し，認証情報の生成を行うことがで，なりすましを用意に行うことができるため問題である．

第 3 章

提案方式

本章では，古田の提案した複数端末認証可能な SAS-2 方式の問題点を解決し，ID/パスワードが漏洩した場合でも，なりすましが困難な複数端末での SAS-2 相互認証方式の提案を行う．また，最後に評価，考察を述べる．

3.1 提案方式の構成

提案方式では，初期登録フェーズ，認証フェーズ，端末登録フェーズで構成される．初期登録フェーズは，1 度だけ実行され，認証フェーズはユーザがログインを行う度に実行される．端末登録フェーズは，ユーザが新たな端末を接続する際に実行する．

3.2 定義と記法

- User は，認証されるユーザである．
- Server は，User を認証する認証者である．
- Uid はユーザの識別子を示す．
- Tid はユーザが使用する端末の識別子を示す
- P はユーザのパスワードを示す．
- SI，SI_A，SI_B は User と Server で共有する乱数を示す．
- SIex は SI_A と SI_B の排他的論理和を示す．
- i は, 認証セッション毎に加算される数値である．
- N_i は，i 回目の認証時に生成される乱数を示す

- Nex_i は，N_i と SI の排他的論理和を示す.
- X，F，H は一方向性関数を示す．例として F(x) は x を一方向性関数に適用して得た出力値を示す．また，この一方向性関数は出力ビット数が常に一定とする.
- +は加算演算子を示す.
- $\oplus$ は, 排他的論理和演算子を示す.
- A,C は認証情報を示す.

3.3　初期登録フェーズ

初期登録フェーズでは，まずユーザが Tid，事前共有乱数 SI，認証情報を生成し，安全な経路を用いてサーバへ共有する必要がある．図 3.1 に初期登録フェーズを示す.

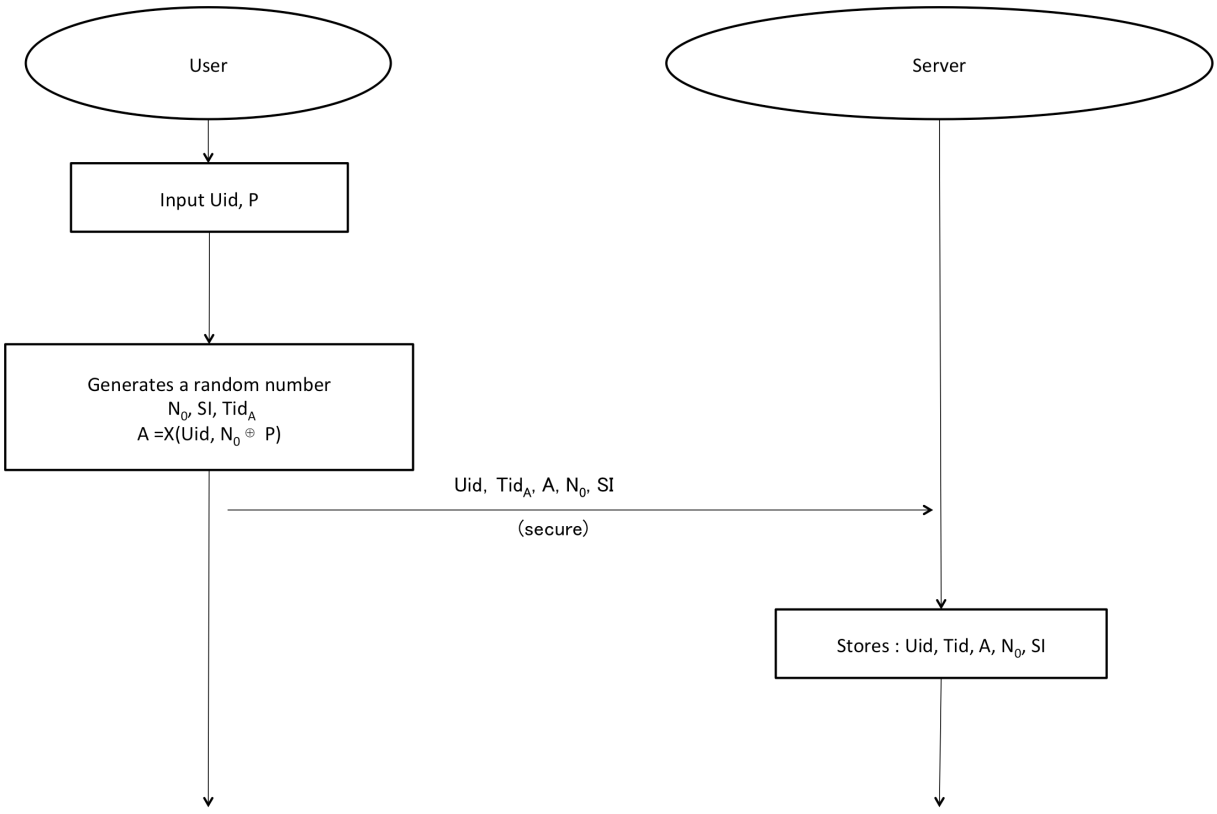

図 3.1　提案複数端末認証可能方式 初期登録フェーズ

1. ユーザは自身の識別情報 Uid とパスワード P を入力する．また，同時に Tid，SI，N_0

の生成を行い，A = X(Uid, P $\oplus$ N_0) を算出する．

2. ユーザは Uid と生成した Tid，SI，N_0，A を安全な経路を用いて送信する．
3. サーバは Uid と Tid,SI，N_0，A を保存する．

3.4 認証フェーズ

認証フェーズでは，まずユーザからレスポンスを送信し，サーバからリクエストをとして秘匿化された乱数を送信する．そして，ユーザが認証情報を生成しサーバへ送信する．サーバが受け取り，認証情報の正当性を検証し，ユーザの認証を行う．次にサーバで認証情報を生成し，ユーザへ送信する．受信した認証情報の正当性をユーザが検証し，サーバを認証する．これにより相互認証が可能となる．i 回目の認証手順を図 3.2 に示す．

1. ユーザは自身の識別情報 Uid とパスワード P を入力する．
2. ユーザはサーバへリクエストとして，Uid と Tid を送信する．
3. サーバは，保存されている N_i と Tid に対応する SI で $Nex_i = N_i \quad \oplus$ SI を算出し，レスポンスとして返信する．
4. ユーザは受信したで Nex_i と端末に保存されている SI を用いて，$N_i = Nex_i \oplus$ SI を算出し，N_i を取り出す．
5. ユーザは Uid と P で N_i，A = X(Uid, P $\oplus$ N_i) を算出する．次にユーザは乱数 N_{i+1} を生成する．そして，ユーザは，C = X(ID, P $\oplus$ N_{i+1}) と F(C) = F(ID, C) を算出し， C,F(C) と A を用いて，α = C $\oplus$ (F(C) + A), β = F(C) $\oplus$ A をそれぞれ算出する． そして，Nex_{i+1}= $N_{i+1} \oplus$ SI を算出する．
6. ユーザは，サーバへ Nex_{i+1}，α，β，を送信する．この時に用いられる通信はインターネットなどの安全でない通信経路であっても構わない．
7. サーバは受信した β と保存されている A を用いて，F(C) = $\beta \oplus$ A を算出し，C = α $\oplus$ (F(C) + A) を算出する．そして，$N_{i+1} = Nex_{i+1}$SI を算出する．次に，$\oplus$F(C) と F(Uid，C) の比較を行う．比較結果が，不一致ならばの認証が不成立となる．一致した

3.4 認証フェーズ

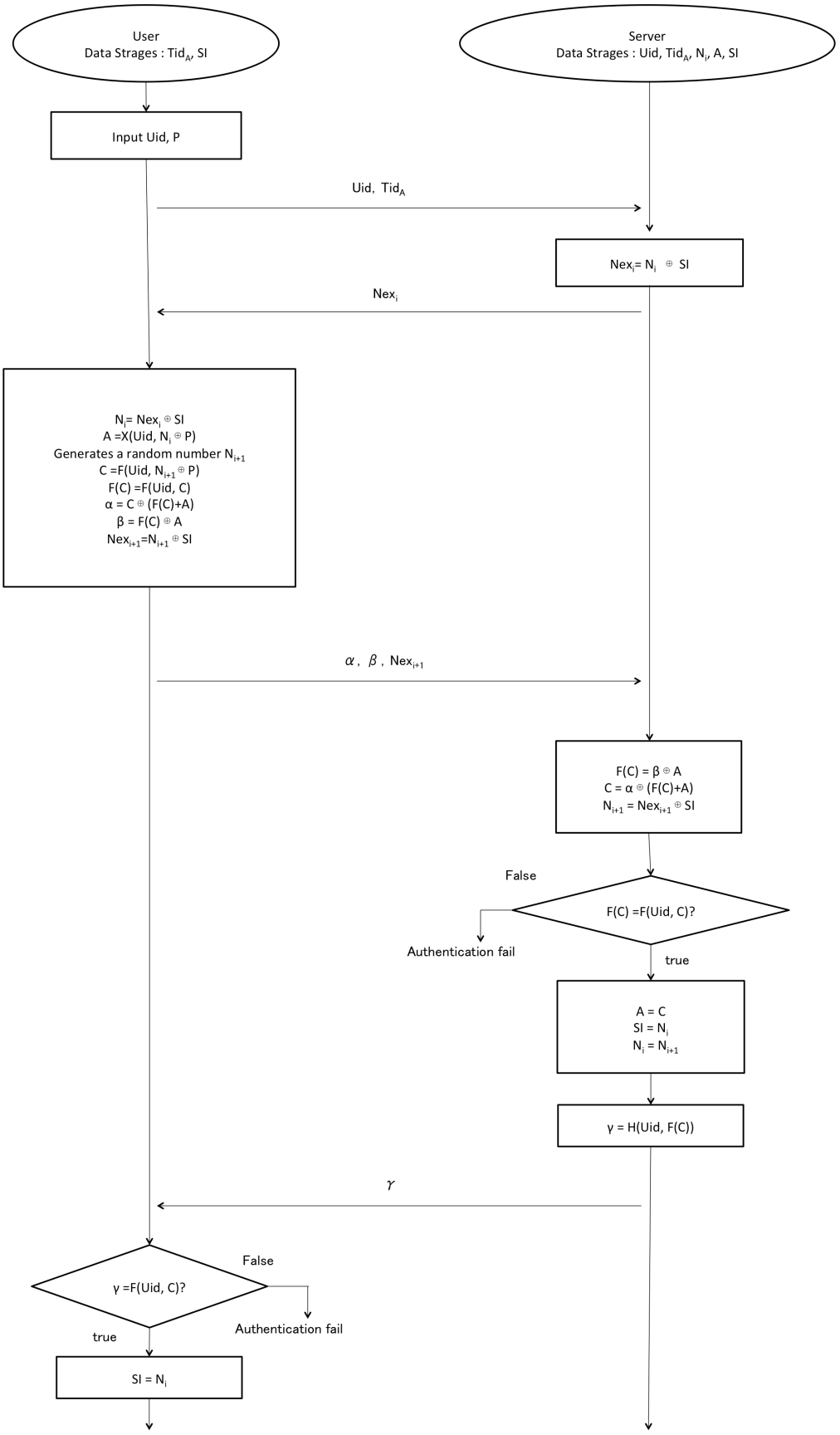

図 3.2　提案複数端末認証可能方式 認証フェーズ

場合は認証が成立となる．認証が成立した場合に以下の処理が実行される．

8. サーバは，保存された A の代わりに C の保存と SI の代わりに N_i を保存，N_i の代わりに N_{i+1} の保存を行い，次回認証に備える．さらに γ = H (Uid $\oplus$ F(C)) を生成し，ユーザへ送信する．この時に用いられる通信はインターネットなどの安全でない通信経路であっても構わない．
9. ユーザは H (Uid $\oplus$ F(C)) を算出し，受信した γ と比較を行う．比較結果が，不一致ならばサーバの認証が不成立となる．一致した場合は認証が成立となる．最後に SI の代わりに N_i を保存する．

3.5　端末登録フェーズ

端末登録フェーズは，相互認証を行い，暗号鍵が生成され，暗号通信が行うことのできる端末を用いて行う．本フェーズでは区別のため，認証済みの端末を A とし，Tid，SI を Tid_A，SI_A とする．また，登録を行う端末を B とし，Tid，SI を Tid_B，SI_B とする．端末登録フェーズの手順を図 3.3 に示す．

1. ユーザは，認証可能な端末で認証フェーズを用いて相互認証を行い，暗号鍵を生成する．
2. SI_B を生成し，端末に保存されるている SI_A で，SIex = $SI_A \oplus SI_B$ を算出し，SIex をサーバへ送信する．
3. サーバは，受信した SIex を保存されている SI_A とで，SI_B = SIex $\oplus$ SI_A を生成する．次に Tid の重複がないように Tid_B を生成する．そして，SI_B と Tid_B をサーバへ保存し，Tid_B をユーザへ送信する．
4. ユーザは受信したで Nex_i と端末に保存されている SI を用いて，$N_i = Nex_i \oplus$ SI を算出し，N_i を取り出す．
5. 最後にユーザの端末で生成した SI_B と受信した Tid_B を表示し，登録を行いたい端末へ共有する．

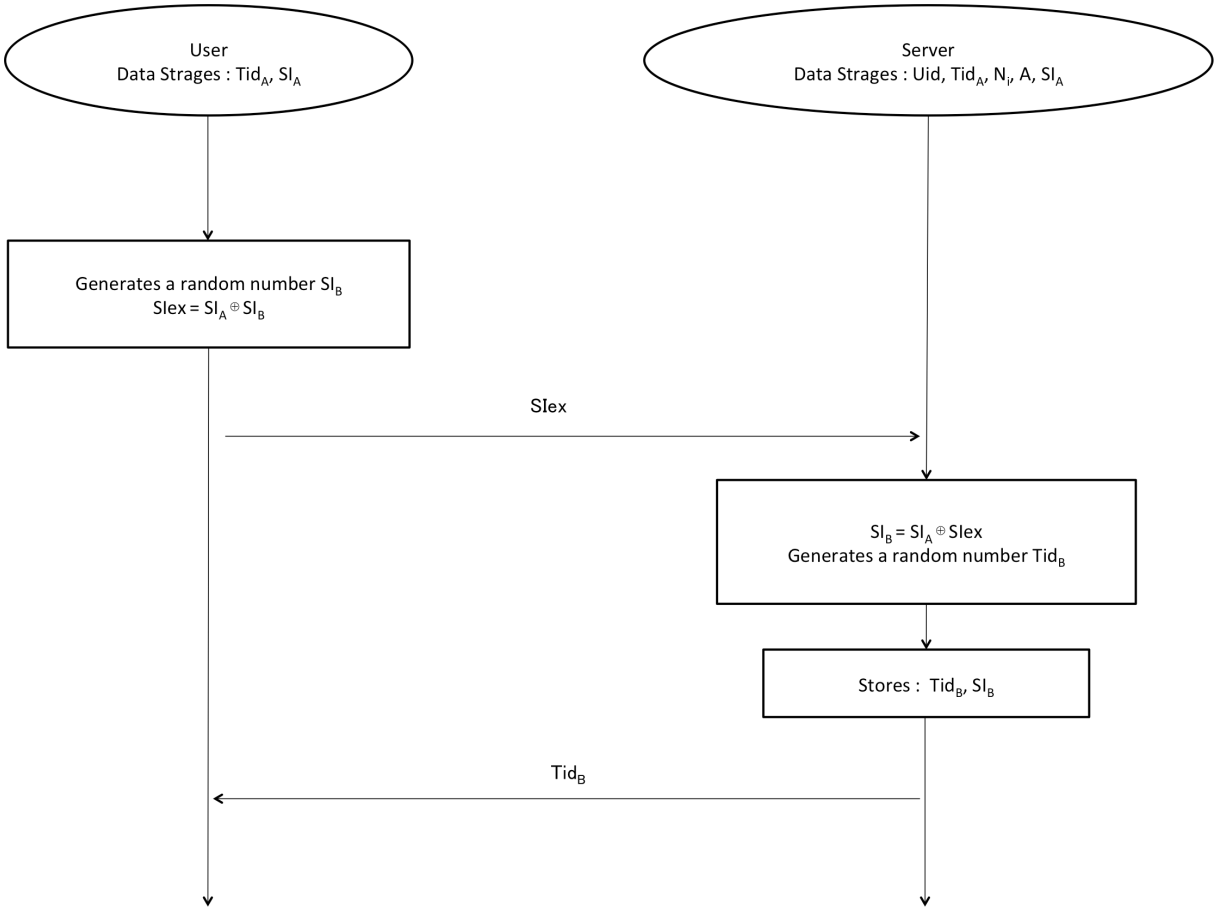

図 3.3　提案複数端末認証可能方式 端末登録フェーズ

3.5.1　方式の安全性

複数端末認証を行う SAS-2 方式に対する攻撃法として，アカウントリスト攻撃によるなりすましがが考えられる．アカウントリスト攻撃では，サービスで用いられる ID/パスワードを不正に取得し，取得した情報を利用して，別のサービスでログインを行う．既存の複数端末認証方式では，乱数をサーバから取得するため，アカウントリスト攻撃を行うことができる．提案方式による i 回目の認証を行う際にされる認証情報生成のための処理を示す．

$$N_i = Nex_i \oplus SIA = X(Uid, P \oplus N_i) \tag{3.1}$$

認証情報生成時に，ID/パスワード知っている第三者が．なりすましを行う場合，通信手順から取得可能な情報として， Nex_i がある．Nex_i は，$Nex_i = N_i \quad \oplus$ SI で算出されるた

め SI を用いて N_i を Nex_i から取得する必要があるが，SI は第三者が取得できないため安全である言える

第 4 章

評価と考察

本章では，提案複数端末認証方式を用いた SAS-VPN の実装を行い，既存の複数端末可能な認証方式と提案方式と認証時間と安全性，保存情報数で比較評価を行う．HTTP 通信と HTTPS 通信と提案方式のリクエスト・レスポンスの処理時間の検証，安全性の評価を行う．また IKE と SSL/TLS を用いた鍵共有方式と提案方式のにおける安全性と共通鍵の共有が行われるまでの通信回数，鍵共有手法の評価を行う．

4.1 実装環境

実装環境を，表 4.1 に示す．

表 4.1 VPN 方式の比較

	クライアント	サーバ
OS	MacOS X Yosemite	CentOS 6.9
CPU	1.3 GHz Intel Core i5	Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz
メモリ	4GB 1600MHz DDR3	1GB
開発言語	java 1.8.0_162-ea	java 1.8.0_25-b17

4.1.1 SAS-2 方式の比較

．表**??**は，遠藤の方式のなかで提案されている SAS-2 方式，既存複数端末可能 SAS-2 方式，複数端末の認証の可否，提案暗号方式の通信回数，一方向性関数の適応回数の比較を行

う．通常の SAS-2 では，端末に乱数を保存するため，複数端末での認証を行うことができ

表 4.2　SAS-2 方式の比較

	複数端末認証可否	通信回数	安全性	一方向性関数		保持情報数	
				ユーザ	サーバ	ユーザ	サーバ
SAS-2	×	2 回	○	4 回	2 回	3	2
既存複数端末認証可能 SAS-2 方式	○	4 回	×	4 回	2 回	2	3
提案複数端末認証可能 SAS-2 方式	○	4 回	○	4 回	2 回	4	5

ない．既存複数端末認証可能 SAS-2 通信では仕乱数をサーバに登録する方式で複数端末認証を可能にした．しかし，既存複数端末認証可能 SAS-2 方式では，ID/パスワードが漏洩した場合になりすましが容易になってしまう．提案複数台数認証方式では，既存複数端末認証可能方式に比べ，排他的論理和と事前共有情報を用いることにより，ID/パスワードが漏洩しても問題のない方式となった．以上のことから従来の 2 つの方式に比べ，複数端末認証による利便性の向上と共に，ID/パスワードの漏洩によるなりすましへの対応を行った複数端末による SAS-2 認証が可能である．

4.1.2　HTTP/HTTPS 通信との評価

表**??**は，1MB，5MB，10MB のデータを HTTP 通信，HTTPS 通信，提案方式を用いて 1000 回取得した平均時間である．検証した結果，HTTP 通信と提案方式を用いた VPN では，通信速度が約 32% 低下した．HTTPS 通信と提案方式では約 16% 低下した．この原因として，通信情報の暗号化や通信経路の増加によるものである．

HTTP 通信では，暗号化を行わないため，安全ではない．

HTTPS 通信では，ユーザがアクセスする Web ページに依存して，HTTPS 通信を行う

表 4.3　各データサイズにおけるリクエスト・レスポンス処理時間 [s]

	1MB	5MB	10MB
HTTP 通信	0.5110	2.5611	5.1294
HTTPS 通信	0.6344	3.2110	6.3953
SAS-VPN	0.7522	3.7889	7.5977

表 4.4　HTTP/HTTPS 通信と SAS-VPN の比較

	暗号化範囲	暗号化適応範囲	安全性
HTTP 通信	暗号化を行わない		×
HTTPS 通信	HTTP データ	対応ページのみ	△
SAS-VPN	送信情報全て	全てのページ	○

ため，対応していないサイトに接続する場合，暗号化を行わない．HTTP データのみ暗号化され，IP ヘッダは暗号化されない．そのため，通信先のサーバを特定することが可能であり，利用者が利用しているサービスを特定することが可能である．また，偽装したアクセスポイントへ接続した場合の偽装ページへのアクセスの問題を防ぐことはできない．

提案方式では，VPN を用いることにより，安全に通信を行うことができる．また，VPN ではアクセスされる Web ページに依存することなく暗号化を行うことが可能である．

4.2　鍵共有方式の評価

共通鍵共有の方式として，IKE，SSL/TLS，SAS-2 がある IKEv2，SSL/TLS，SAS-VPN では，様々な暗号化方式を用いれるため，安全に通信を行うことができる．IKEv2 は IPsec，L2TP/IPsec など OS に標準搭載されているため容易に接続が可能である．OpenVPN，SAS-VPN では，クライアントソフトのインストールする必要がある．しかし SAS-VPN では，証明書を用いて認証を行わないため，証明書の管理コストを省くことができる．また，IKE や SSL/TLS では，共通鍵の共有過程で共有鍵生成情報の暗号化を行う必要があ

表 4.5 鍵共有方式の比較

	代表的な方式	安全性	証明書の必要性	利便性
IKEv2	IPsec-VPN L2TP/IPsec	○	必要	○
SSL/TLS	OpenVPN	○	必要	△
SAS-2	SAS-VPN	○	不要	△

り，SAS-2 では用いる必要がない．そのため，証明書用いることなく相互認証を行えるため，証明書の管理コストを削減した VPN 通信が可能となる．

4.3 考察

評価の結果から，既存の SAS-2 方式，既存複数端末 SAS-2 方式に比べ，サーバと端末上に保存する情報が増加した．しかし，複数端末認証を行える，ID/パスワードが漏洩しても安全である点で優れていると言える．HTTP 通信，HTTP 通信に比べ，低速になってしまっている．しかし，偽装アクセスポイントに接続しても安全である点，Web ページに暗号化が依存しない点が優れているといえる．鍵共有方式では，クライアントソフトが必要になるため，公開鍵を証明するための，証明書を用いることなく相互認証を行える点が優れているといえる．

提案する複数端末認証可能 SAS-2 方式では，SI を用いて，送信されるの乱数の秘匿がされる．しかし，排他的論理和を用いておこなっており，ブルートフォース攻撃を用いて解読されてしまう可能があるため，SI の安全なデータサイズを検証する必要がある．

第 5 章

結論

近年，多くの公共施設で公衆無線 LAN サービスが提供されている．しかし公衆無線 LAN サービスはノンパスワード，共通パスワード，偽装 SSID の問題がある，その問題を対策として，遠藤によるワンタイムパスワード認証方式 SAS-2 を用いた VPN サービスが提案された．しかし他の VPN 方式や HTTPS 通信との比較がされていない．また，複数端末認証が不可能であるため，安全に複数端末認証方式を提案した．提案方式では事前共有情報 SI を用いることにより，ID/パスワードの漏洩があった場合でも，なりすましを困難にする．また SAS-VPN の評価を行い，他の VPN サービス, HTTPS 通信との比較をし優れている点を示した．今後の展望として，提案する複数端末認証可能 SAS-2 方式では，SI を用いて，送信されるの乱数の秘匿がされる．しかし，排他的論理和を用いておこなっており，ブルートフォース攻撃を用いて解読されてしまう可能があるため，SI の安全なデータサイズを検証する．

謝辞

本研究の遂行及び論文作成にあたり，言葉では言い表せないほどの御指導，御助言を賜わた高知工科大学情報学群 清水明宏教授に心より感謝し厚く御礼申し上げます.

本研究の副査を担当していただいた高知工科大学情報学群 吉田真一准教授，植田和憲講師に深く御礼申し上げます.

また，本学大学院修士課程 藤田寛康氏には，研究内容について有益なアドバイスをいただき，心より感謝いたします．最後に，有益な議論を交わしていただいた高知工科大学セキュリティシステム研究室の関係者各位に深く感謝いたします.

参考文献

[1] 株式会社 ICT 総研，“2017 年度公衆無線 LAN サービス利用者動向調査,” 2017.

[2] 総務省，“H28 年度総務省 ICT 関係重点政策,” 2016.

[3] T.Tsuji, and A.Shimizu, “Simple And Secure password authentication protocol Ver.2 (SAS-2),” IEICE Technical Reports, OIS2002-30，2002.

[4] 遠藤 俊，“SAS-2 による VPN を用いたセキュアな公衆無線 LAN サービスの提案,” 高知工科大学 情報学群，2016.

[5] 古田 千春，“SAS-2 における複数端末認証の研究，” 高知工科大学大学院 工学研究科 基盤工学専攻 情報システム工学コース，2015.

[6] 独立行政法人情報処理推進機構，“公衆無線 LAN 利用に係る脅威と対策,”, 2016.

[7] 平井圭佑，菊池浩明，“偽装証明書を用いたファーミング攻撃の危険性について,” 東海大学 情報通信学部,2012

[8] Charlie Scott，Paul Wolf, Mike Erwin，“VPN 第 2 版”，オライリー・ジャパン，2002.

[9] S.Kent，K.Seo，“Security Architecture for the Internet Protocol RFC4301,” IETF, 2005.

[10] K.Hamzeh，G.Pall， W.Verthein，J.Taarud，W.Little and G.Zorn， “Point-to-Point Tunneling Protocol (PPTP) RFC 2637,” IETF, 1999.

[11] W.Dixon，G.Zorn，S.Booth，“Securing L2TP using IPsec RFC 3193,” IETF, 2001.

[12] J.Schiller， “Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2) RFC 4307” IETF, 2005.